31

THE HARMON MEMORIAL LECTURES
IN MILITARY HISTORY

NUMBER THIRTY-ONE

United States Air Force Academy
Colorado
1988

THE INTELLIGENCE REVOLUTION: A HISTORICAL PERSPECTIVE

Sir Harry Hinsley
Master
ST. JOHN'S COLLEGE, CAMBRIDGE

D 305.10:

READEX FICHE best copy available

For a complete listing of previous Harmon lectures see pages 11 & 12.

Views or opinions expressed or implied in this publication are those of the author and are not to be construed as carrying official sanction of the Department of the Air Force or of the United States Air Force Academy.

THE INTELLIGENCE REVOLUTION: A HISTORICAL PERSPECTIVE

Sir Harry Hinsley
Master
St. John's College, Cambridge

THE HARMON MEMORIAL LECTURES
IN MILITARY HISTORY

NUMBER THIRTY-ONE

United States Air Force Academy
Colorado
1988

For sale by the Superintendent of Documents, U.S. Government
Printing Office, Washington, D.C. 20402

THE HARMON MEMORIAL LECTURES
IN MILITARY HISTORY

COMMITTEE

CHAIRMAN: Colonel Carl W. Reddel, USAF
Professor of History
U.S. Air Force Academy

MEMBERS: Harold C. Deutsch
Retired

John F. Guilmartin, Jr.
Associate Professor of History
Ohio State University

Richard H. Kohn
Chief, Office of Air Force History

EXECUTIVE SECRETARY: Captain Donald B. Hondrum, USAF
Instructor of History
U.S. Air Force Academy

Lieutenant General

Hubert Reilly Harmon

FOREWORD

The Department of History, United States Air Force Academy, is the sponsor of this lecture series. The purpose of the series is twofold: to help promote a greater knowledge of military history in the United States and abroad; and to stimulate our cadets toward developing a lifelong interest in this, their professional subject.

Each year a committee of internationally known civilian historians and Academy representatives selects an outstanding military historian or a first-rate scholar from a closely related field who, as Harmon lecturer, is invited to present an original lecture on a subject of his choice within the broadly-construed field of military history. In keeping with the purpose of the series, the lecture is published and distributed to leading scholars and libraries throughout the world.

These lectures are known collectively as the "Harmon Memorial Lectures in Military History," in memory of the accomplishments of the late Lieutenant General Hubert R. Harmon, the first Superintendent and "Father" of the Academy. General Harmon's lifelong personal interest in military history makes it particularly appropriate that he be honored in this way.

Professor Sir Harry Hinsley presented the thrity-first lecture in this series on Wednesday evening, 12 October 1988, to members of the Cadet Wing, members of the faculty, and distinguished guests attending the Thirteenth Military History Symposium, "The Intelligence Revolution: A Historical Perspective." His presentation served as a fitting keynote address for the Symposium.

Sir Harry Hinsley has combined a remarkable career as an educator with a unique and personal viewpoint on intelligence. Born on 26 November 1918, Sir Harry received his early education at Queen Mary's Grammar School. He interrupted his studies at St. John's College, Cambridge, to serve at the Government Code and Cypher School at Bletchley Park. His work there brought him into close contact with most of the other British intelligence organizations during World War II.

After the war Sir Harry completed his M.A. at St. John's College and became Lecturer in History, Cambridge University. He later served as Professor, History of International Relations, St John's College, Cambridge; Lees-Knowles Lecturer on Military Science, Trinity College, Cambridge; and Vice-Chancellor, Cambridge University. His major publications include: *Command of the Sea*, (1950), *Hitler's Strategy*, (1951), *Power and the Pursuit of Peace*, (1963), and *British Intelligence in the Second World War: Its Influence on Strategy And Operations*, (jointly) 4 volumes, 1979-88.

Sir Harry Hinsley is presently Master of St. John's College, Cambridge, and a Trustee of the British Museum. He was awarded the Order of the British Empire in 1945 for wartime service in the Foreign Office, and was knighted by Queen Elizabeth II in 1985.

THE INTELLIGENCE REVOLUTION: A HISTORICAL PERSPECTIVE

Harmon Memorial Lecture U.S. Air Force Academy

12 October 1988

Sir Harry Hinsley

In the Second World War, if we leave aside the information they obtained by overt means from embassies, the press, the radio and other such channels, governments received their intelligence from four sources:

1. Physical contact in the form of captured documents, the censorship of mail and the interrogation of prisoners;
2. Espionage;
3. Aerial reconnaissance, particularly aerial photographic reconnaissance; and
4. Signals intelligence, SIGINT for short.

About these four sources we should note two preliminary points. Essentially, each of them had always existed. There never was a time when governments did not avail themselves of censorship, captures, prisoners and spies; aerial reconnaissance was old-fashioned reconnaissance greatly extended by the development of flying since the beginning of this century; SIGINT, in the same way, was the product of the marriage of one of the most ancient of crafts—cryptanalysis—with the advent of wireless communication. In the second place, all governments exploited all these sources in World War II or did their best to do so.

To this extent the outbreak of the war was not at once followed by an intelligence revolution, and this was all the more the case because until the autumn of 1941—for the first two years of the war—the intelligence bodies on both sides achieved roughly equal success or failure. To illustrate this point by reference only to SIGINT, the most valuable and prolific of all the sources, British success in breaking the cypher used by the Germans in the April 1940 invasion of Norway and in reading the Luftwaffe's communications after May 1940 was balanced by the fact that the Germans read between 30 and 50 percent

of British naval traffic in the North Sea and the Atlantic during 1940, and a considerable amount of the French Army's traffic from the outbreak of war to the fall of France. That the British were reading the high-grade cyphers of the Italian Army, Navy and Air Force from September 1940 to the end of 1941 was offset by Axis successes during most of that period against equivalent British cyphers in the Mediterranean and Middle East.

Axis successes against British cyphers did not cease at the end of 1941. From January 1942 to June 1943 Germany continued to read many of the codes and cyphers associated with the Atlantic convoys. However, the previous rough equivalence of advantage in SIGINT gave way in the autumn of 1941 to massive Allied superiority. It did so in a process by which Axis openings were successively blocked, and the Allied penetration of Axis communications, and especially of German communications, was progressively expanded. It was expanded to a degree that had never been achieved before, even in wartime. Leaving aside the decryption of tactical codes and cyphers—confining ourselves to the highest grade decrypts for which London used the code-name *Ultra* and Washington used the code-names *Ultra* and *Magic*—the Allies were reading from the end of 1942 between 3,000 and 4,000 German signals a day and a large, but somewhat smaller, volume of Italian and Japanese traffic. Whereas to Germany, Italy, and Japan virtually all the Allied cyphers had by then been made invulnerable.

While SIGINT, as a result of the development of radio, was for the first time in history the most prolific as well as the most reliable intelligence source, and since the possession of it made it possible to maximize the benefits and minimize the defects of the other sources, the scale of this transformation enabled intelligence to exercise an unprecedented influence on the course and outcome of the war. In the longer term, as a direct consequence of that experience, it had a profound and permanent effect on the status and the organization of intelligence. Intelligence is unlikely ever again to return to the age of innocence—to that condition of general neglect interspersed with bursts of belated and amateur endeavor in times of crisis—that had characterized it to the middle of the twentieth century.

How, then, was the transformation brought about? In answering this question nothing is more striking than the extent to which both fortune and foresight, both good luck and good judgment, played their part.

This point is best illustrated by the long and tangled history of that achievement which was most central to the transformation—the conquest of the German Enigma machine.

The Enigma was Germany's answer to the problems raised by their wish to utilize radio in military operations most effectively. Impregnable cyphers as well as the capability to cypher and decypher large volumes of confidential signals were necessary. To achieve the advantages of mass production, Germany chose to rely almost exclusively on a single electro-mechanical typing machine, called Enigma, distributing it widely throughout each of the three services and within such other organizations as the *Abwehr* (the German counterintelligence service), the railways, and the police. By each of its user organizations, however, the machine was adapted to different arrangements and procedures, and each of them operated it with different keys for different functions and in different theaters. Some 250 keys, each constituting a different cypher, were identified during the war, and at no time after 1941 were less than fifty in force concurrently. Because each key was reset daily once war had begun, and as the finding of any setting involved the selection of one out of many millions of possible solutions, the Germans had good reason to feel confident that even in war conditions the Enigma would remain safe against all but local and temporary compromise. And yet the machine was basically, if not irretrievably, compromised as early as 1932, and beginning in May 1940 after an interlude since September 1938, the Allies went on to recover over 180 wartime keys and to read German traffic almost currently.

The prewar compromise owed almost everything to chance or, as the Germans might think, to misfortune. The Poles broke the machine by methods that involved great mathematical ingenuity, but the methods were possible only because in 1931 a German signals officer supplied its operating instructions and settings for periods of some length to the French Secret Service, which passed them to Warsaw. But fortune played a much less central part in the wartime conquest of the Enigma.

The Polish success had been brought to an end in 1938 by the last in a sequence of prewar German security improvements. Despite the invaluable assistance obtained from the Poles, and that from September 1939 the Germans used the machine more heavily in operational conditions, whereas they had previously used it sparsely and mainly for practice traffic, the British did not fully solve any wartime keys—to bring them to the point at which the settings were found daily without

great delay—until the spring of 1940, when they mastered the key used in Norway from 10 April and the Luftwaffe's general purpose key from 20 May. Many regional and specialized Luftwaffe keys were thereafter solved, often as soon as they were brought into force; but it is further testimony to the formidable problems presented by the Enigma that no naval keys were solved regularly before June 1941, and no Army keys (with the exception of one on the Russian front from June 1941) till the spring of 1942. Nor need we doubt that but for careful preparations over a long period of time the British authorities would not, even then, have overcome these problems.

Without their foresight in centralizing cryptanalysis on an inter-departmental basis after World War I, in recruiting the best available talents to it from 1938, and not least in recognizing that those talents should be inter-disciplinary, the conquest of the Enigma would have been impossible. And while it would have been impossible without brilliant mathematicians, and particularly without their development of machinery of a sophistication the Germans had not allowed for, it would equally have been impossible without the input of a whole array of non-mathematical ingenuity.

These successes once achieved could not be counted on to continue. They were subject to two threats. The Germans, who had made successive improvements to the security of the Enigma before the war, might continue to do so as a matter of ordinary precaution. Or they might refashion it from suspicion or conviction that it had been radically compromised. Under the pressures of war and in view of the unexpected wide dispersal of their armed forces, the German authorities, with one notable exception, deferred routine precautionary measures until after the middle of 1944. Not until early in 1945, when the Enigma was daily vulnerable to physical compromise, did they take measures in the belief that it was no longer secure. The exception was the U-boat Command. In February 1942, motivated initially by suspicion—which was, however, set aside after a professional inquiry—it took the precaution of bringing into force a new Enigma key, one that used an additional wheel and was 26 times more difficult to solve.

The effects of this setback, and of those originating from the burden of solving the ever increasing proliferation of ordinary keys, were offset, though with remarkably small delay, by another of the great developments of World War II. From the spring of 1942 the British and American intelligence bodies created for SIGINT, as for other

forms of intelligence, a single organization in which the amalgamation of resources and the division of labor were virtually complete. This joint effort was necessary to sustain success against the Enigma. And as the Allies wrestled after the autumn of 1944 with Germany's adoption of increasingly severe security measures, they had to fear that not even their combined resources would suffice to maintain their critical advantage. As a result of Germany's delay in producing either precautionary measures or drastic revisions, the Allies kept their advantage, and even extended it, down to the end of the war.

It is tempting to attribute this incredible delay by the Germans to their undue confidence in the invulnerability of the Enigma before the war, and to their incompetence and complacency after the war began. But there are good grounds for holding that their original confidence was not unreasonable, and that to think otherwise is to belittle the ingenuity and the versatility of the Allied SIGINT effort. These capabilities were displayed against Japanese and Italian cyphers as well as against Germany's, and against other German cyphers besides the Enigma—most notably against the system Germany introduced for communication between her high-level headquarters in a signaling system based on teleprinter impulses that were automatically cyphered and decyphered on transmission and at the point of reception. The British had broken this system even before it was fully operational, by developing an approximation to the modern computer. Thus, the argument for wartime German incompetence overlooks some important considerations which must be taken into account if one is to understand the intelligence revolution in this war.

In continuing to make no allowance for the development of machine methods against the Enigma, the Germans were undoubtedly swayed by their own inability to make any progress against Allied machine cyphers and the fact that they had no opportunity to capture them. The danger that they might believe the Enigma had become insecure, if only as a consequence of captures, was contained until almost the end of the war by, on the one hand, the existence of the other intelligence sources and, on the other, exceptionally careful Allied precautions. Oblivious to the Allied possession of *Ultra*, but knowing that, like themselves, the Allies exploited the other sources, they attributed to prisoners, deserters, spies or treachery the setbacks they encountered as a result of SIGINT—and all the more so because they were fighting alongside unreliable allies in occupied countries with hostile populations.

The Allies also utilized this situation to conceal their reliance on *Ultra* from their own forces by citing the other sources as the basis for operational orders inspired by SIGINT. Concealment from their own forces, however, was only one part of the meticulous system of precautions the Allies evolved to avert the enemy's attention from the use they were making of *Ultra* intelligence in their operations.

At some stages in the war—as it happens, with the assistance of Italian machine decrypts as well as of Enigma decrypts—the British were sinking 60 percent of the Axis shipping that plied between the European Mediterranean ports and North Africa, but no Axis ship was attacked before the enemy had learned that it had been sighted by an aircraft or warship which, unknown to itself, had been put in a position to make the sighting. There were occasions on which, to the alarm of the Allied authorities, the procedures broke down—when orders were issued that referred to the intelligence or when a cover was not provided for the action that might result. There were also situations to which these precautions could not be applied. In the Atlantic, in particular, there was a long period in which the decrypts of the instructions to U-boats, though used to great effect, were used only passively, to route convoys out of the path of U-boats rather than to steer the escorts to where the U-boats were waiting or refueling. In such a situation, in which more and more U-boats made fewer and fewer sightings, the mere absence of sightings of convoys was bound to create enemy suspicions as happened in the German U-boat Command in early 1942. In order to lull German suspicions the Allies utilized such methods as exaggerating the extension of Allied air reconnaissance to the mid-Atlantic and by propagating a rumor that the Allies had invented a miraculous radar which detected submerged U-boats over great distances. The planting of this type of cover had to be very carefully controlled but without these tremendous efforts to keep the secret, while maximizing its use, the situation would have been different.

Against these considerations it may be argued that if the Allied precautions were effective it was only because, like all successful deception measures, they buttressed known convictions, and that Germany's assumptions and blindspots must still be attributed in the last resort to undue confidence and profound carelessness. But it is necessary to guard against hindsight. The war by this time had seen a revolution—at least in the amount, the continuity, the reliability, and the currency of intelligence. This undermined Germany's security to

an unparalleled extent, but, unlike the Allies, the Germans did not know that the transformation had taken place. Moreover, the Allies were not entirely shielded against overconfidence. Although they were benefiting from the revolution, they did not realize that the Germans were reading their convoy cyphers until, from the end of 1942, the truth was revealed by explicit references in the Enigma decrypts of the instructions being issued by the U-boat Command to their U-boats. And while this confirms that it is a counsel of perfection to preach that it is unwise to be confident about anything, ever, it also raises a further question. What was the value of all this mass of intelligence? If its existence could remain undetected for so long, can its influence have been decisive, as is so widely believed?

In addressing this question it is important to distinguish between the impact of intelligence on the course of operations and, on the other hand, its strategic value.

As every commander and any intelligence officer knows, intelligence is only one among many elements affecting the course of operations. It is necessary to consider much else when reaching decisions, and many other factors besides the decisions affect the outcome. For these reasons the operational impact of intelligence was always variable, not to say haphazard, even if it was far less so than had previously been the case.

It was especially so up to the summer of 1941 when, as well as giving roughly equal advantage to both sides, intelligence was limited in volume and usually obtained with some delay, if obtained at all. Although claims to the contrary have been made, few British operations before that date benefited from intelligence. With photographic aerial reconnaissance, but without assistance from other sources, the authorities were able in the autumn of 1940 to time their bombing of the concentrations of invasion barges in the Channel so as to obtain maximum effect. In the winter of 1940-1941 the British were able to mitigate the ferocity of the Blitz with the help of SIGINT, prisoners of war and equipment recovered from crashed enemy aircraft. In the spring of 1941, thanks to advance warnings from SIGINT, the *Bismarck* was sunk at the beginning of her cruise, whereas the *Graf Spee* had been caught at the end of a long sortie without any benefit from intelligence at all. Also, that same spring the Royal Navy intercepted the Italian Fleet and defeated it at the battle of Cape Matapan, with a slight amount of SIGINT. In Crete the defending force inflicted a severe mauling on

the German airborne invaders. The operational achievements of intelligence were increasing, but they remained few in number.

After the summer of 1941, in contrast, most battles or sizable encounters in the European and Mediterranean theaters, with the possible exception of the Russian front, were influenced by the Allied superiority in intelligence, especially by the sheer volume of current decrypts. But the contribution made by intelligence was by no means always important, let alone decisive. Random factors like luck or misjudgment were sometimes uppermost. A great deal was known about the enemy's intentions when convoy PQ-17 sailed for Murmansk in June 1942, but the convoy still ran into disaster. On the other hand, the sinking of the *Scharnhorst* in the Arctic on the day after Christmas 1943 was almost wholly brought about because intelligence, though small, became crucial when the enemy made mistakes. Sometimes relative strength settled the question. In the first battle of El Alamein in June-July 1942 intelligence about the Africa Corps was not yet plentiful, but it was decisive in enabling the British commander to prevent Rommel's greatly superior armor from breaking through to Cairo—despite the fact that Rommel was better supplied with field intelligence. Before and during the second battle of El Alamein in October 1942 the amount of intelligence about Rommel's forces was massive, but those forces were by then so inferior to Montgomery's that it played little part in the British victory.

It would be very wrong, however, to assess the significance of intelligence for the outcome of the El Alamein battles by measuring only its direct impact on them. What limited Rommel's superiority before the summer of 1942, and helped to eliminate it by the autumn, was the British use of SIGINT to destroy his supply shipping. Axis losses, rising to a peak of over 60 percent of southbound Mediterranean shipping in November 1941 and to another peak between 50 and 60 percent in October 1942, were almost entirely attributable to decrypts of cypher keys that had been solved regularly since June 1941. Nor was this the only direction in which the transformation of the intelligence situation to the advantage of the Allies now laid the basis for the indirect, long-term, strategic effects that intelligence was to exercise till the end of the war. Also from June 1941, for the first time, the British read the U-boat traffic regularly and currently, an advance that almost wholly explains why they prevented the U-boats from

dominating the Atlantic during the autumn of 1941 and the winter of 1941-1942.

What, then, was the overall influence of intelligence on the war? It is not easy to give a precise assessment. If its impact on individual operations was not always decisive, and was sometimes nil, its strategic impact was indirect and cumulative. It is thus difficult to measure it now, as it was difficult for the enemy to discern it at the time. But two conclusions may be advanced without qualification. In the first place, the claim that intelligence by itself won the war—a claim that is self-evidently absurd—may be dismissed. The British survived with little benefit from it before Germany invaded Russia in June 1941, as the Russians survived invasion with little benefit from it; and as Russia's survival was followed by the entry of the United States in December 1941, the Axis would have been defeated even if the Allies had not acquired by that date the superiority in intelligence they retained till the end of the war. Till the end of the war? Nearly four more years is such a length of time that it might be thought that, far from not producing on its own the Axis defeat, intelligence made little contribution to it. That this was not the case, however, is the second point that may be made without qualification.

The war effort of the Western Allies on every front after the end of 1941 was guided by massive, continuous and frequently current information about the enemy's dispositions, intentions, resources and difficulties. The information was so comprehensive, though never complete, that, though the Allies occasionally misinterpreted it, the expectations they based on it, whether positive or negative, were generally correct. This enabled them not only to strike some decisive operational blows and avoid some operational setbacks, but also to shorten the war by setting the time, the scale and the place of their own operations in such a way as to achieve enormous economies for themselves in lives and resources and to add enormously to the burdens the enemy had to bear.

By how much did the Allied superiority in intelligence shorten the war? Even if the question is limited to the war in Europe the answer can only be approximate. By keeping the Axis out of Egypt it probably brought forward the conquest of North Africa and the reopening of the Mediterranean to Allied shipping, which were completed in the middle of 1943, by at least a year. By preventing the U-boats from dominating the Atlantic in the winter of 1941-1942, and by contributing heavily

to their defeat there in the winter of 1942-1943, it probably saved the Allies another two years. Had delays of this order been imposed by shortages of shipping and specialized landing craft on the Allied invasions of the Continent, those undertakings would have been further delayed by other considerations. As it was, the invasion of Normandy was carried out on such very tight margins in 1944 that it would have been impracticable without precise intelligence about German strengths and orders of battle and the fact that the Allied commands could be confident the intelligence was accurate. If it had had to be deferred it might well have been delayed beyond 1946 or 1947 by Germany's V-weapon offensive against the United Kingdom and her ability to finish the Atlantic Wall, not to speak of her deployment of revolutionary new U-boats and jet and rocket aircraft which, as intelligence revealed, became imminent by the end of 1944. At best, the return to the Continent might have been delayed till 1948 and the defeat of Germany till 1949, and that is probably a conservative estimate.

Neither the Western Allies nor the Russians would have been idle in these circumstances. What different strategies would they have pursued? Would the Russians have defeated Germany, or Germany the Russians? What would have been decided about the atom bomb? Historians cannot answer these questions, because fortunately they are concerned only with the war as it was. And it was not least because of the actual contribution made by intelligence to the course of the war that such horrible questions did not arise.

PREVIOUS HARMON MEMORIAL LECTURES

I. *Why Military History*, by W. Frank Craven, 1959

II. *The Military Leadership of the North and the South*, by T. Harry Williams, 1960

III. *Pacific Command*, by Louis Morton, 1961

IV. *Operation Pointblank*, by William R. Emerson, 1962

V. *John J. Pershing and the Anatomy of Leadership*, by Frank E. Vandiver, 1963

VI. *Mr. Roosevelt's Three Wars: FDR as War Leader*, by Maurice Matloff, 1964

VII. *Problems of Coalition Warfare: The Military Alliance against Napoleon*, by Gordon A. Craig, 1965

VIII. *Innovation and Reform in Warfare*, by Peter Paret, 1966

IX. *Strategy and Policy in Twentieth-Century Warfare*, by Michael Howard, 1967

X. *George C. Marshall: Global Commander*, by Forrest C. Pogue, 1968

XI. *The War of Ideas: The United States Navy, 1870-1890*, by Elting E. Morison, 1969

XII. *The Historical Development of Contemporary Strategy*, by Theodore Ropp, 1970

XIII. *The Military in the Service of the State*, by General Sir John Hackett, G. C. B., C. B. E., D. S. O., M. C., 1971

XIV. *The Many Faces of George S. Patton, Jr.*, by Martin Blumenson, 1972

XV. *The End of Militarism*, by Russell F. Weigley, 1973

XVI. *An Enduring Challenge: The Problem of Air Force Doctrine*, by I. B. Holley, Jr., 1974

XVII. *The American Revolution Today*, by John W. Shy, 1975

XVIII. *The Young Officer in the Old Army*, by Edward M. Coffman, 1976

XIX. *The Contribution of the Frontier to the American Military Tradition*, by Robert M. Utley, 1977

XX. *The Strategist's Short Catechism: Six Questions Without Answers*, by Philip A. Crowl, 1978

XXI. *The Influence of Air Power upon Historians*, by Noel F. Parrish, 1979

XXII. *Perspectives in the History of Military Education and Professionalism*, by Richard A. Preston, 1980

XXIII. *Western Perceptions and Asian Realities*, by Akira Iriye, 1981

XXIV. *Command Crisis: MacArthur and the Korean War*, by D. Clayton James, 1982

XXV. *United Against: American Culture and Society During World War II*, by John M. Blum, 1983

XXVI. *George Washington and George Marshall: Some Reflections on the American Military Tradition*, by Don Higginbotham, 1984

XXVII. *Military Planning and National Policy: German Overtures to Two World Wars*, by Harold C. Deutsch, 1984

XXVIII. *Napoleon and Maneuver Warfare*, by Steven T. Ross, 1985

XXIX. *Soldiering in Tsarist Russia*, by John L.H. Keep, 1986

XXX. *Leadership In The Old Air Force: A Post-Graduate Assignment*, by David MacIsaac, 1987

UNITED STATES AIR FORCE ACADEMY

Provides instruction and experience to each cadet so that he or she graduates with the knowledge and character essential to leadership and with motivation to become a career officer in the United States Air Force.